COMPUTER VIRUSES & WORMS

Gavin Schiavi

What is a Computer Virus/Worm?

- A computer virus is a type of computer program that replicates itself by modifying other computer programs and inserting its own code.
- A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers.

- It often uses a computer network to spread itself, relying on security failures on the target computer to access it.

- It will use this machine as a host to scan and infect other computers.

How Do They Work?

- Computer viruses generally require a host program. The virus writes its own code into the host program.

- When the program runs, the written virus program is executed first, causing infection and damage.

- A computer worm does not need a host program, as it is an independent program or code chunk. Therefore, it is not restricted by the host program, but can run independently and actively carry out attacks.
- A viable computer virus must contain a search routine, which locates new files or new disks that are worthwhile targets for infection. Secondly, every computer virus must contain a routine to copy itself into the program which the search routine locates.

Why Are They Used?

- Seeking profit with Ransomware: a type of malicious software designed to block access to a computer system until a sum of money is paid
- Send a political message
- Personal amusement
- Demonstrate a vulnerability in software
- Sabotage and denial of service
- Explore cybersecurity issues, artificial life and evolutionary algorithms

HOW ARE VIRUSES AND WORMS PREVENTED?

Anti-Virus Software

- Antivirus software detects and removes computer viruses

How Do Anti-Virus Software's Work?

- Database with known malicious software

- Cross-check files in a database to identify Viruses in your system.

- Anything not in the database, or anything that obscures the signature’s paper trail, can slip through the system.
- Malware samples are analyzed by malware researchers or by dynamic analysis systems. Then, once it is determined to be a malware, a proper signature of the file is extracted and added to the signatures database of the antivirus software.

What Do They Prevent?

- Modern antivirus software can protect users from malicious browser hijackers, ransomware, backdoors, worms, fraud tools, and spyware.
- Some products also include protection from other computer threats, such as spam, scam and phishing attacks, online identity, online banking attacks, social engineering techniques, DDoS attacks.

How Coding Applies

- To stay ahead of Virus software, Malware authors write their own viruses (oligomorphic, polymorphic and metamorphic), which encrypt parts of themselves or otherwise modify themselves as a method of disguise, so as to not match virus signatures in the dictionary.

- These codes are extremely complex, translating their own binary code into a temporary representation, editing the temporary representation of themselves and then translating the edited form back to machine code again.